UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------x

UNITED STATES OF AMERICA, :
v. :
: Indictment No.
: 15-cr-866 (WHP)
ROGER THOMAS CLARK,
:
Defendant.
:

----------x

MEMORANDUM OF LAW IN SUPPORT OF MOTION TO SUPPRESS AND FOR DISCOVERY

Stephanie M. Carvlin
Jacob Mitchell
Counsel for Roger Thomas Clark
140 Broadway, Suite 4610
New York, New York 10005
212-748-1636

TABLE OF CONTENTS

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES

Federal Statues

Cases

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------x

UNITED STATES OF AMERICA, :
v. :
: Indictment No.
: 15-cr-866 (WHP)
ROGER THOMAS CLARK,
:
Defendant.
:

----------x

PRELIMINARY STATEMENT

Roger Thomas Clark is charged in this case for his purported role, under the pseudonyms "Variety Jones" or "VJ" and "Cimon" in helping to run Silk Road. Silk Road was a website that during its operation provided a platform for users to purchase drugs and other illegal goods and services online. In an attempt to obtain evidence against the individuals who were behind Silk Road, the government conducted warrantless searches in the United States of a servers[1] that hosted the website. The searches were conducted in violation of the Fourth Amendment to the United States Constitution. This Memorandum of Law is submitted in support of Roger Thomas Clark's motion to suppress the direct results of the unconstitutional searches of the server, to suppress all evidence that was obtained derivatively from those searches (the "fruits"), to suppress evidence obtained through torture and to obtain additional discovery.

[1] A computer server is a host computer that sends data to and receives data from client computers and or other servers. (Declaration of Joshua L. Michel at 6, n7.)

STATEMENT OF FACTS

Silk Road began to operate in January of 2011. On June 1, 2011, *Gawker*, a media outlet, published a story online about the website. Days later, New York Senator Charles Schumer held a press conference condemning Silk Road and urging the Drug Enforcement Administration ("DEA"), and the Justice Department to close the site down. By 2013, federal law enforcement agencies, including the Secret Service, the Federal Bureau of Investigation ("FBI"), Homeland Security Investigations ("HSI"), the Internal Revenue Service ("IRS") and the DEA in Chicago, Baltimore and New York had begun investigations to try to locate Silk Road. Over the 18 months following Senator Schumer's calls to close the site, the government had made little progress in determining who ran Silk Road. Law enforcement was under intense pressure to bring the website down.

By February of 2013, the government, through means it has never disclosed, and still refuses to disclose, located what it believed to be the Internet Protocol ("IP")[2] address of the Silk Road computer server with IP address 193.107.84.4 (".4"). That IP address corresponded to a server in Iceland. [redacted]

[2]Internet Protocol is the method by which data is sent from computer to computer on the Internet. Internet Protocol address is a unique series of 32 numbers that identifies each device that sends or receives information over the Internet. The location of a computer or other electronic device can be determined through the device's IP address. (Michel Declaration at ¶1.)

[redacted](Exhibit 1 to Declaration of FBI Special Agent Christopher Tarbell dated September 5, 2014, attached as Exhibit C to Declaration of Jacob B. Mitchell, "Mitchell Declaration.") In May of 2013, Icelandic authorities produced traffic data for the .4 server to the FBI. (Tarbell Declaration at 5, n7, Exhibit C to Mitchell Declaration.)

[redacted]Tarbell Declaration at Exhibit 1 page 1, Exhibit C to Mitchell Declaration).[redacted]

That IP address – the .49 address – ostensibly was discovered by FBI Special Agent Christopher Tarbell, and another member of CY-2, the cybercrime squad of the FBI's New York field office, sometime in June of 2013. In a Declaration Agent Tarbell submitted in the government's prosecution of Ross Ulbricht in this District,[3] the agent asserted that he and an unidentified fellow agent located the .49 IP address as follows: The Silk Road website was accessible only through Tor - The Onion Router - an Internet browser that encrypts data and then transmits it randomly through multiple relays or nodes. The last node appears as the origination point of the data, thereby obscuring and making it impossible to determine the actual IP address of the sender. To access Silk Road a user would have to download the Tor software. Once in the Tor browser, someone who wanted to access Silk Road would type in the Tor, or .onion,

[3] *United States v. Ross Ulbricht*, 14-cr-68 (KBF).

address for Silk Road, which would call up the login page. The user would then enter a registered username and password and complete the CAPTCHA[4] field. (Tarbell Declaration at ¶¶4-5, Exhibit C to Mitchell Declaration.) According to Agent Tarbell, he and the unidentified fellow CY-2 agent ran a series of tests to try to locate the Silk Road IP address sometime in "early June" of 2013." They accessed the Silk Road login page (through Tor) and entered both random invalid information and valid user credentials, which corresponded to undercover accounts members of law enforcement had established on the site. (*Id.* at ¶7.) Using some unspecified software or device, the agents then "closely examined" the individual packets,[5] or component parts of the data, that were sent back in response to their entries. This activity is known as "packet sniffing." (Declaration of Joshua L. Michel, "Michel Declaration" at 2, n2.)

When a non-Tor browser, such as Google Chrome, is used packets display the IP addresses of the source and destination computers that were used to route the packets over the Internet. Conversely, if a computer is properly set up to run Tor, any IP addresses should appear as an IP address of a Tor node thereby cloaking the true IP address of the device that sent the packets. (Tarbell Declaration at ¶¶4-5, Exhibit C to Mitchell Declaration.) According to Agent Tarbell, one of the IP addresses he and the other CY-2 agent found while accessing Silk Road through Tor was not associated with

---

[4]CAPTCHA is an acronym for Completely Automated Public Turing. A CAPTCHA is a "test" that that is designed to tell if the user is a human or an automated service. Generally, it consists of typing a series of letters that are revealed or selecting designated types of images from a series – bridges, crosswalks, etc.

[5] Data sent over the Internet is broken into manageable units, or "packets", which are reassembled when received at the destination. (Michel Declaration at ¶4.)

any known Tor node.[6] Agent Tarbell concluded that the non-Tor IP address might be the true IP address of the Silk Road server, which had "leaked", that is, become visible, "because the computer code underlying the login interface was not properly configured at the time to work on Tor." (Tarbell Declaration at ¶8, Exhibit C to Mitchell Declaration.) Agent Tarbell asserted that he entered the non-Tor IP address he had discovered into a regular Internet browser, and the Silk Road CAPTCHA prompt appeared. (*Id.*)

[redacted]

[6]There is a publicly available list of known Tor nodes. (Tarbell Declaration at 4, n4, Exhibit C to Mitchell Declaration).

[7]Agent Tarbell was certified as a Forensic Computer Examiner by both the FBI and the International Association of Computer Investigative Specialists ("IACIS") (Tarbell Declaration at ¶3, Exhibit C to Mitchell Declaration). The IACIS defines computer forensics as "the acquisition, authentication, reconstruction, examination, and analysis of data stored on electronic media." http://www.iacis.com/core competency).

[redacted]

Those lines of computer code do not show that Silk Road's IP address had leaked in the manner Agent Tarbell claimed. (Michel Declaration at ¶31.)

[redacted]

[redacted][8]

The contents of the .49 server were analyzed by agents of the FBI in the United States without obtaining a search warrant. "From examining the computer code on the Silk Road Server, the FBI learned of IP addresses of additional servers used in connection with administering the Silk Road website."(Government's Memorandum of Law in Opposition to Defendant's Motion to Suppress filed in *United States v. Ulbricht*, 14-cr-68 (KBF), Exhibit H to Mitchell Declaration at 4.) The government first uncovered a backup server at a data center in Pennsylvania. (*Id.*) Based on information it initially obtained through its search of the .49 server, the government ultimately applied for and received search warrants for that backup server,[9] for a secondary backup server in Pennsylvania,[10] for a Tor-bridge server in Pennsylvania,[11] for a Bitcoin wallet back-up server,[12] and for two servers in California.[13] Relying on information derived from the FBI's analysis of the .49 Iceland server, the government made requests pursuant to Mutual Legal Aid Treaties ("MLATs") or similar diplomatic protocols for images of the

[8]In the Ulbricht prosecution the government stated that it would not rely on the contents of the Silk Road server that were obtained as a result of the June 6, 2013 imaging of the .4 server. Given that the government in this prosecution has not turned over a copy of the June 6, 2013 image of the .4 computer, it is apparent that it will take the same position in this case.

[9]September 2013 warrant on Windstream Data Center; September 2013 warrant on JTAN.com; October 2013 warrant on Windstream Data Center for IP address 207.106.6.25.

[10] October 2013 warrant on Windstream Data Center for IP address 207.106.6.32.

[11] October 2013 warrant on Windstream Data Center for IP address 207.106.6.11.

[12]September and October 2013 warrants for IP address 109.163.234.40.

[13]IP addresses 109.163.234.40, IP 109.163.234.37.

contents of a Silk Road private-key server[14] and a Silk Road discussion-forum server that were located in France and Iceland, respectively.[15] In September and October of 2013, the government requested that Iceland reimage the .49 server and the Silk Road Bitcoin wallet server in Iceland.[16]

Law enforcement's review of the contents of the Silk Road server led directly to the government's identification of Ulbricht as Dread Pirate Roberts, the originator of Silk Road.[17] Using the information derived from the .49 server, the government obtained warrants to search Mr. Ulbricht's residence, which yielded, *inter alia*, a USB thumb drive, a Kindle, and a Samsung laptop. On the laptop the government found records Mr. Ulbricht kept in connection with his administration of Silk Road, including a journal that chronicled notable events in the development of the site, and logs of expenses Mr. Ulbricht incurred in running the site. The laptop also contained a 1500-plus page document that the government asserts is a "Tor-chat log" that supposedly contains written exchanges between Dread Pirate Roberts ("DPR") – Ross Ulbricht – and Variety Jones/Cimon, who the government asserts is Mr. Clark.

---

[14]A private key – a series of random letters and numbers - is used in conjunction with a public key – a different series of random letters and numbers as part of an encryption process designed to secure communications made over the Internet. To initiate a secure communication an individual obtains both a private and public key and provides only the public key to others. Those individuals use the public key to send their communications, which can be de-encrypted only by the holder of the private key.

[15]IP addresses 62.75.246.20 and 82.221.104.28.

[16]IP address 193.107.86.34.

[17]As the government stated previously in its opposition to Ross Ulbricht's motion to suppress the contents of the Icelandic server, "Ross Ulbricht did not even become a suspect in the FBI's investigation until well after the SR Server was searched." (Government's Response to the Declaration of Joshua J. Horowitz, Exhibit E to Mitchell Declaration at 6.)

The government applied for and received orders on September 16, 19, and 20, 2013, permitting it to use a Pen Register and Trap and Trace device to obtain information about devices purportedly associated with Ross Ulbricht. Through actions taken pursuant to these orders the government was able to collect routing data associated with Mr. Ulbricht's Internet traffic, particularly the IP addresses to which those devices associated with him connected to the Internet and the dates, times and duration of those connections.

Ross Ulbricht was arrested on October 1, 2013, in San Francisco, California. He was indicted in this District on February 4, 2014. The government superseded the indictment on August 21, 2014, leading to a total of seven charges against Mr. Ulbricht: narcotics trafficking in violation of 21 U.S.C. §§841(a)(1) and (b)(1)(A), distribution of narcotics by means of the Internet in violation of 21 U.S.C. §§841(b)(1)(A) and 841(h), narcotics trafficking conspiracy in violation of 21 U.S.C. §§841(b)(1)(A) and 841(h), continuing criminal enterprise in violation of 21 US.C. §848(a), conspiracy to commit and aid and abet the commission of computer hacking in violation 18 U.S.C. §1030(b), conspiracy to traffic in fraudulent identification documents in violation of 18 U.S.C. §1028(f) and conspiracy to commit money laundering in violation of 18 U.S.C. §1956(h). On February 5, 2015, Mr. Ulbricht was convicted, following trial, on all seven counts.

In April of 2015, the United States Attorney's Office in the Southern District of New York [redacted]

[redacted]

On April 21, 2015, a criminal complaint was filed in this District, charging Mr. Clark with conspiring to distribute narcotics in violation of 21 U.S.C. §§841(b)(1)(A) and 846 and with conspiring to launder money in violation of 18 U.S.C. §1956(h). (15-Mag-1335). The complaint alleged that Mr. Clark was Variety Jones (VJ), a/k/a Cimon, and he had been involved in running the Silk Road website. Specifically, the government alleged that Mr. Clark was responsible for the following:

a. Hiring and managing a computer programmer who assisted in developing computer code and maintaining Silk Road's technical infrastructure;

b. Providing advice to Ulbricht regarding managing and operating Silk Road, including security advice, and advice regarding the rules and policies on Silk Road;

c. Assisting in promoting sales on the Silk Road website, including providing help with coordinating a large-scale promotion for the sale of narcotics and other contraband on Silk Road; and

d. Conducting research and collecting intelligence on the efforts of law

enforcement to investigate Silk Road.

(15 Mag. 1335 at 7.) A warrant was issued for Mr. Clark's arrest the same day.

At the request of the United States, authorities in Thailand, where Mr. Clark was then residing, provisionally arrested him on December 3, 2015, on the charges recited in the complaint. During the arrest, the Royal Thai Police seized a variety of digital devices from Mr. Clark's residence: a silver and black Acer Aspire laptop (serial number NXM2RST013223110F1200); a silver MacBook Pro laptop (serial number C02HN0WNDV7P), a black Hewlett Packard Presario CQ60 with USB dongle inserted (serial number 2CE843138V), a Seagate Barracuda LP hard drive (Serial number 5YD265A1), a black and blue Transcend thumb drive (8 GB), two Micro Center USB flash drives (32 GB) and a dark grey Olympus *fe* camera (serial Number J7I20910). During their arrest of Mr. Clark, agents of the Royal Thai Police demanded that he sign a form – in Thai – indicating that he consent to seize the articles. When he refused they repeatedly beat him with sticks until he signed the form, marking it "not read or understood, signed under duress." (Declaration of Roger Thomas Clark at ¶23).

Discovery turned over by the government in this case documents that on December 4, 2015, immediately preceding his arraignment in court in Thailand, Mr. Clark was interviewed by Special Agent Michael Joseph of HSI. Agent Joseph advised Mr. Clark of his *Miranda* rights orally and in writing. Mr. Clark agreed to waive his rights, and the two spoke for a brief period before Mr. Clark was taken to Court. Mr. Clark wrote two letters to Agent Joseph thereafter. The men met in person again on May 11, 2016, while Mr. Clark was being held in custody pending his extradition to the United States. Mr. Clark made additional statements to Agent Joseph.

An amended complaint was filed in the Southern District of New York on December 17, 2015. The government added four additional charges against Mr. Clark: narcotics trafficking in violation of 21 U.S.C. §841(b)(1)(A), distribution of narcotics by means of the Internet in violation of 21 U.S.C. §§841(b)(1)(A) and 841(h), conspiracy to commit and aid and abetting the commission of computer hacking in violation of 18 U.S.C. §1030(b) and conspiracy to traffic in fraudulent identification documents in violation of 18 U.S.C. §1028(f).

In 2015, the government filed a sealed indictment against Mr. Clark in this District. This indictment remains sealed, and the government has not provided a copy to the defense. The controlling indictment – S1 15 Cr. 866 (WHP) – was filed on January 17, 2018. It charges Mr. Clark with the six offenses contained in the amended complaint.

On June 15, 2018, Mr. Clark was extradited to the United States from Thailand. Discovery provided by the government in this case documents that after Mr. Clark's arrival at the courthouse in the Southern District of New York, he declined to be interviewed by law enforcement, asserting that he would rather wait for counsel. However, during a conversation with FBI Special Agent Samad Shahrani, Mr. Clark offered that he was looking forward to quitting smoking, which he would have to do in light of the no-smoking policy in federal prisons in the United States. Agent Shahrani advised Mr. Clark that he would likely still be able to get cigarettes while incarcerated. Mr. Clark responded that he thought it was ironic for someone in his position, but he did not like to use black markets.

ARGUMENT

POINT ONE

BY SEARCHING THE CONTENTS OF THE SILK ROAD SERVER IN THE UNITED STATES WITHOUT A WARRANT THE GOVERNMENT VIOLATED THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION

The Fourth Amendment guarantees individuals the right to be secure in their "persons, houses, papers and effects against unreasonable searches and seizures[.]" A search or seizure protected by the Fourth Amendment occurs in two circumstances: when law enforcement infringes on an individual's subjective expectation of privacy that society is prepared to recognize as reasonable; *Katz v. United States*, 389 US 347, 361, 88 S. Ct. 507, 516 (1967)(Harlan, J., concurring); and when law enforcement conducts a physical intrusion into a constitutionally protected area in a manner that would constitute a common-law trespass. *United States v. Jones*, 565 U.S. 400, 405, 407 (2012). By searching in the United States the computer servers that powered the Silk Road website the government violated Mr. Clark's subjective and objectively reasonable expectation of privacy.[18]

1. Mr. Clark Demonstrated a Subjective Expectation of Privacy in the Contents of the Icelandic Servers

An individual shows the requisite subjective expectation of privacy to challenge a search by demonstrating "a subjective desire to keep his or her effects private." *United States v. Paulino*, 850 F.2d 93, 97 (2d Cir. 1988); *See Palmieri v. Lynch*, 392 F.3d 73, 81 (2d Cir. 2004)(by erecting a fence, posting a "No Trespassing" sign and writing

[18]A defendant has the burden of establishing that the challenged searches and seizures violated his own Fourth Amendment rights. *Rakas v. Illinois,* 439 U.S. 128 (1979).

letters indicating his refusal to consent to a search of his property, the land owner demonstrated a subjective expectation of privacy in the area). In the Declaration he has submitted in support of this motion, Mr. Clark affirms that he had a subjective expectation of privacy in this material. (Clark Declaration at ¶20.) His assertion is indisputably true. Mr. Clark's actions are proof that he intended to and wanted to keep the IP address, location and contents of the Icelandic servers private.

As Mr. Clark states in his Declaration, user could enter the Silk Road website only by using the Tor browser. The purpose of using Tor, as the government notes in the complaint it filed in this case, is to make it "practically impossible to physically locate the computer hosting or accessing websites on the network." (15 Mag. 1335 at ¶21 a.) All purchases made through Silk Road had to be paid for in Bitcoin, an anonymous currency. (Id. at ¶21 b.) Silk Road used a Bitcoin tumbler to process the Bitcoin transactions "in a manner designed to frustrate the tracking of individual transactions[.]" (Id. at ¶21 k.) Additionally, as Mr. Clark affirms in his Declaration, he advised DPR on how to configure the website's code to prevent others from gaining unauthorized access to the server. (Clark Declaration at ¶6.)

Mr. Clark's implementation and use of these and other security measures demonstrate that Mr. Clark had an actual subjective expectation of privacy in the non-public contents of the .49 server.[19] He wanted the information to remain private, and he believed that it would remain private. *See United States v. Long*, 64 M.J. 57, 63 (C.A.A.F. 2006)(affirming lower court's finding that by using a password not known to

[19]The images of the .49 server that the government obtained document how the Silk Road website existed on the date the images were captured. This includes components of the site that were available to the public – the marketplace, the forums and the wiki pages.

the system administrator, a member of the Marine Corp demonstrated a subjective expectation of privacy in emails she sent from her office computer and emails that were stored on the government server); *United States v. Loera*, 333 F.Supp.3rd 172, 183 (E.D.N.Y. 2018)(concluding that by encrypting his communication network so as to prevent interception the defendant demonstrated a subjective expectation of privacy in the communications made on the system); *United States v. Howe*, 2011 WL 2160472, at *7 (W.D.N.Y. May 27, 2011)(Defendant's use of password protection on the computer he rented demonstrated that he had a subjective expectation of privacy in its contents).

2. Mr. Clark's Expectation of Privacy Was Objectively Reasonable

Mr. Clark's expectation of privacy in the Iceland servers was objectively reasonable. In the Declaration Mr. Clark has submitted in support of this motion he affirms that he had an ownership interest in the Silk Road website business. (Clark Declaration at ¶16). The United States Supreme Court has held that Fourth Amendment protection applies to searches or seizures in commercial establishments, as well as in residences. An individual indisputably may contest the search of his own office. *Mancusi v. DeForte, 392 U.S. 364, 369 (1968);* and the owner or operator of a business "has an expectation of privacy in commercial property, which society is prepared to consider to be reasonable." *New York v. Burger,* 482 U.S. 691, 699, 601 (1987).

While a search for data (in electronic devices, in emails, in records maintained by third parties) presents more complex Fourth Amendment issues, several rules are clear. Individuals possess a reasonable expectation of privacy in the contents of their home computer; *United States v. Lifshitz,* 369 F.3d 173, 190 (2d Cir.2004); and an employee who has exclusive use of an office computer, even if the device is owned by his

employer, has a reasonable expectation of privacy in that computer. *Leventhal v. Knapek*, 266 F.3d 64, 73 (2d Cir. 2001). Fourth Amendment protection arises because of the connection the defendant has to the information stored on the computer. As required by the case law that forms the foundation of the Supreme Court's Fourth Amendment jurisprudence, a defendant who is asserting that his own electronic data is searched without proper justification is asserting a violation of his own Fourth Amendment rights. *Rakas*, 439 U.S. at 140 (the proper inquiry is whether the disputed search or seizure has "infringed an interest of the defendant which the Fourth Amendment was designed to protect").

The courts that have considered what a defendant must show to establish a cognizable Fourth Amendment interest in a computer server have held, consistent with the rules that have historically been applied with respect to brick-and-mortar searches, that an individual must assert he had a "personal connection" to the electronic files stored on the server. *United States v. Nagle*, 803 F.3d 167, 178 (3d Cir. 2015); *United States v. Mendlowitz*, 2019 WL 1017533, at *5-7 (S.D.N.Y. Mar. 2, 2019). A defendant "may make such a showing by asserting that he owned or leased the premises (for example, the leasing of a server would count) or had dominion or control over them. [*United States v.*] *Watson*, 404 F.3d [163, 166 (2d Cir. 2015]; *United States v. Villegas*, 899 F.2d 1324, 1333 (2d Cir. 1990)." (Order and Opinion, *United States v. Ulbricht*, 14-cr-68 (KBF), at 15, Exhibit J to Mitchell Declaration.)

The government has labeled Mr. Clark alternatively as Mr. Ulbricht's "mentor" or "trusted advisor" or "employee." However, these characterizations are inconsistent with the description of Mr. Clark's role the government provided in warrant applications, in its

request to Thailand seeking his extradition, in the complaint filed in this case and in submissions filed in the Ulbricht prosecution. In those documents, the government attributed a far more key role to Mr. Clark:

- Mr. Clark advised Ross Ulbricht regarding managing and operating Silk Road, including security advice and advice regarding the rules and policies. The two communicated regularly – almost daily, often for several hours a day, for a period of more than two years – about all aspects of the operation and management of the Silk Road website.

- He recommended and then instituted security improvements to the website designed to make the servers more secure from outside penetration.

- He located, hired and managed the computer programmer who redesigned Silk Road's code and maintained Silk Road's technical infrastructure.

- He insisted that Mr. Ulbricht enforce a requirement that all order information be encrypted.

- He recommended methods to enforce the requirement that sales take place within Silk Road's escrow system, which Mr. Ulbricht adopted.

- He designed and implemented sales promotions.

- He ran security for the site, conducting research and intelligence on law enforcement's efforts to penetrate the site. When an administrator of the site stopped communication, Mr. Clark offered to find the man and determine what had happened.

These are not the actions of an employee.

As he states in his Declaration, Mr. Clark's initial contact with Silk Road was as a user of the website. However, his role evolved over time to the point that he was responsible for helping DPR run all aspects of the site, as the government itself asserts as the basis for this prosecution. Mr. Clark hired and fired employees. He fundamentally changed the design (physical appearance and technical structure) of the website. He fought with DPR over policies governing how to organize the core feature of the website that made it viable– the escrow system. More often than not, Mr. Clark's view prevailed.

(Clark Declaration at ¶15.) Mr. Clark often advanced his own funds to pay employees' salaries or to purchase hardware needed to improve the functioning or security of the site. (Clark Declaration at ¶12.) While DPR sometimes transferred Bitcoins to Mr. Clark to reimburse him for these expenditures, DPR did not always do so. Rather, the two had an agreement that Mr. Clark was investing in the business and would receive an ownership interest in return. He did not receive a salary like Silk Road employees did. (Clark Declaration at ¶13.)

By February 2013, when the .4 Silk Road IP address (193.107.84.4) was inexplicably discovered, Mr. Clark had an owner and operator interest in Silk Road. He maintained that interest through "early June, 2013," when the United States government asked the RMP to image the .49 server, through July 23, 2013, when the images of the .49 and .20 (62.75.246.20) servers were made and throughout the period during which members of law enforcement searched those servers in the United States. Roger Clark had a personal connection with the electronic files. He took efforts to keep them private.

The fact that Mr. Clark did not pay the fee for the rental of the server does not undermine his assertion that he had a reasonable expectation of privacy in its contents. *See*, *e.g.*, *Byrd v. United States*, 584 U.S. ---, 138 S.Ct. 1518 (2018)(defendant who was lawfully driving a rental car but was doing so in violation of the rental car agreement still had reasonable expectation of privacy in the contents of the trunk); *United States v. Buckner,* 473 F.3d 551, 554 n. 2 (4th Cir. 2007) (user of leased computer had a reasonable expectation of privacy in password-protected files); *Rakas v. Illinois*, 439 U.S. at 142-43 ("[A] person can have a legally sufficient interest in a place other than his own home so that the Fourth Amendment protects him from unreasonable

governmental intrusion into that place."); *Mancusi v. DeForte*, 392 U.S. at 368 (the Fourth Amendment "does not shield only those who have title to the premises.") .

Mr. Clark's Declaration demonstrates that he had a subjective and objectively reasonable expectation of privacy sufficient to permit him to raise a Fourth Amendment challenge to the government's actions.

3. The Government's Failure to Obtain A Warrant to Search in the United States Data Obtained from the Icelandic Server Violated the Fourth Amendment

If a defendant meets the burden of showing that he had a subjective and objectively reasonable expectation of privacy in the material searched, "the government has the burden of showing that the search was valid because it fell within one of the exceptions to the warrant requirement." *United States v. Perea*, 986 F.2d 633, 639 (2d Cir. 1993). The government cannot meet this burden in this case. Unless one of a few "specifically established and well-delineated exceptions" applies, a warrantless search is unreasonable under the Fourth Amendment. *Katz v. United States*, 389 U.S. at 357. No exception to the warrant requirement justified the government's failure to obtain a warrant to search in the United States the images of the .49 and .20 servers that the Icelandic authorities provided on or about July 29, 2013, September 2013, and October of 2013.

Admittedly, the warrant requirement of the Fourth Amendment does not apply to searches or seizures that occur outside of the United States. *United States v. Lee*, 723 F.3d 134, 139 (2d Cir. 2013). It has no extraterritorial application. *In re Terrorist Bombings of U.S. Embassies in East Africa*, 522 F.3d 157, 168-71 (2d Cir. 2008). This rule acknowledges the simple reality that the United States government cannot insist

that a foreign government operate according to the Constitution and laws of the United States. *Id.* at 171. Additionally, the purpose of the exclusionary rule is to provide a deterrent effect: if members of law enforcement know that any evidence they obtain illegally will not be admissible, they have a reduced incentive to violate a person's constitutional rights. When application of the exclusionary rule will not deter official misconduct – as it would not when applied to the conduct of foreign officials – the purpose behind the rule loses its justification. *United States v. Janus*, 428 U.S. 433, 454 (1976).

Mr. Clark's motion does not contest the imaging of the servers in Iceland but the subsequent warrantless searches of the contents of the servers in the United States. This required a search warrant, as the government implicitly acknowledged by obtaining warrants to search the contents of the United States servers in Pennsylvania and in California. Under these circumstances – where the searches at issue took place in the United States and the possibility of obtaining a warrant was readily available to the government – suppressing the evidence would have the deterrent effect the exclusionary rule is designed to foster.

The contents of the .49 and .20 servers and any other servers that were searched in the United States must be suppressed.

4. The Fruits of the Warrantless Searches Must be Suppressed Also

The government's failure to seek a warrant to authorize the United States-based searches of the server images mandates that the evidence obtained directly as a result of those warrantless searches be suppressed. Evidence that is a "product of the primary evidence, or that is otherwise acquired as an indirect result" of the constitutional

violation must also be suppressed. *Murray v. United States*, 487 U.S. 533, 537 (1988); *See United States v. Hearn*, 496 F.3d 236, 234 (6th Cir. 1974)("information gained by law enforcement officers during an illegal search cannot be used in a derivative manner to obtain other evidence").

In this case, virtually all of the evidence the government obtained following the imaging of the servers obtained from Iceland was uncovered by exploiting the original Fourth Amendment violation. As the government admitted in a filing it made in connection with the Ulbricht prosecution it was through examination of the computer code on the .49 server "that the FBI learned of the IP addresses of additional servers used in connection with administering the Silk Road website." (Exhibit H to Mitchell Declaration at 4.) The "reality is that the FBI did not learn of the Silk Road backup servers in the United States until after reviewing the images of the SR Server provided by Icelandic authorities, which was found to contain references to the IP addresses of such other servers." (*Id*. at 11.) In fact, in establishing probable cause for the warrants to search those servers, for the warrant to search Mr. Ulbricht's residence and laptop, for the warrant to obtain the contents of the Weigand email account, for the warrant to search the electronic devices seized from Mr. Clark's residence in Thailand and for the Pen Register and Trap and Trace Orders directed to devices associated with Ross Ulbricht, the government recited and relied on the information it got from examining the contents of the .49 servers.

All this evidence, and testimony about this evidence, must be suppressed. *See Silverman v. United States*, 365 U.S. 508 (1961)(the exclusionary rule prohibits the

introduction of evidence seized during an unlawful search and testimony about that evidence).

POINT TWO

AGENTS OF THE FBI CONDUCTED A SEARCH SUBJECT TO THE REQUIREMENTS OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION BY "EXAMINING" THE PACKET DATA SENT FROM THE SILK ROAD SERVER.

Federal Bureau of Investigations Special Agent Christopher Tarbell affirmed in the Declaration he submitted in the Ulbricht prosecution that he and an unidentified fellow member of the FBI CY-2 squad in New York City discovered the IP address of the .49 Silk Road server by making entries into the Silk Road login page and then examining the packets of data that were returned. (Tarbell Declaration at ¶6-8, Exhibit C to Mitchell Declaration.) The government asserts that through this process, known as "packet sniffing," the agents discovered the second IP address for a Silk Road server."[20] Packet sniffing is a search protected by the Fourth Amendment to the United States Constitution and constitutes an interception of an electronic communication within the meaning of the Federal Wiretap Act. The FBI was required to obtain a warrant to obtain the data.

[20]As noted *supra* at 2, 6-7, unidentified agents of laws enforcement, through unexplained means, discovered an IP address for the server that was powering Silk Road in February of 2013 – the .4 server. The government has refused to disclose how it located that IP address. Agent Tarbell asserts that his discovery of the .49 IP was completely independent of any examination of the contents of the .4 server. (Tarbell Declaration at 5, n7, Exhibit C to Mitchell Declaration.)

1. **By Obtaining Content Information Through Packet-Sniffing Without a Warrant the FBI Violated the Electronic Communications Privacy Act and Conducted a Search that is Protected by the Fourth Amendment**

While agent Tarbell's Declaration is vague on this point, it is clear that his packet sniffing revealed the contents of the .49 server. Data sent through the Internet is broken into "packets" – or bits – that consist of header bits and payload bits. (Michel Declaration at ¶4.) The header contains the source and destination IP addresses, and other information that is needed to get the data from Point A to Point B. The payload is the data to be transported.[21] For example, the contents of an email would be the payload. The IP address of the sending and receiving computers would be part of the header. (*Id.* at ¶4.) A "packet sniffer" or "packet analyzer" is a software program or piece of hardware that captures, records and analyzes packets as they are being transmitted between computers or between a computer and a computer server. (*Id.* at 2, n2.) By packet sniffing to obtain the contents of the packet information sent from the Silk Road server, Agent Tarbell violated the Electronic Communications Privacy Act ("ECPA").

Pursuant to § 2511(1)(a) of the ECPA, part of the Federal Wiretap Act, any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" commits a felony. Intercept is defined as "the aural or other acquisitions of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical or other device." 18 U.S.C. §2510(4). A computer is a device within the

[21]Agent Tarbell affirmed that he and his fellow agent examined the individual packets of data sent back from the Silk Road website and "noticed" the headers of some packets reflected non-Tor IP addresses. He does not say what portions of the packets he examined.

meaning of the ECPA. *United States v. Szymuskiewica*, 622 F.3d 701, 707 (7th Cir. 2010)(computer and computer server constitute devices under 18 U.S.C. § 2510(4)).[22] The packets sent to and from the Silk Road server constitute electronic communications, which are defined as "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce[.]"[23] Thus, by packet sniffing, Agent Tarbell and another member of CY-2 intercepted (used a device to acquire the contents) an electronic communication (a transfer of data) in violation of the ECPA. *See Joffe v. Google*, 746 F.3d 920, 923 (9th Cir. 2013)(affirming District Court's decision not to dismiss lawsuit brought against Google under the Wiretap Act based on the company's packet sniffing of unsecured Wi-Fi networks).

Agent Tarbell's actions also constituted a search under the Fourth Amendment. As detailed *supra* at 13, a search occurs when a member of law enforcement commits a common law trespass or violates a subjective expectation of privacy that society recognizes as reasonable. *Kyllo*, 533 U.S. at 33. Mr. Clark has demonstrated a subjective expectation of privacy in the contents of the Silk Road servers for the

---

[22] Electronic, mechanical or other devices is defined as any "device or apparatus which can be used to intercept a wire, oral, or electronic communication[ ]" other than any telephone or telegraph instrument, equipment or facility or hearing aid. 18 U.S.C. 2510(5).

[23] Certain types of transmissions, not relevant here, are excluded from the definition: wire or oral communications, communications through a tone-only pager, communications from a tracking device and electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

reasons detailed *supra* at Point One and in his Declaration. His expectation of privacy is one that society is today prepared to recognize as reasonable.

While few reported decisions discuss the Fourth Amendment implications of packet sniffing, cases that have analyzed the government's use of similar technology are instructive. In *United States v. Lambis*, 197 F.Supp.3d 606 (S.D.N.Y. July 12, 2016), the defendant argued that law enforcement's warrantless use of a cell-site simulator to locate a cellphone inside his apartment violated the Fourth Amendment. As part of its investigation into an international drug ring, members of the DEA sought and received a warrant for pen register and cell-site location information ("CSLI") for a target cell phone. Through use of the CSLI agents were able to determine only the general area where the phone was located. To try to obtain more specific information, the DEA used a cell-site simulator, a device that "locates cell phones by mimicking the service provider's cell tower (or 'cell site') and forcing cell phones to transmit pings to the simulator." *Id.* at 609. The simulator enabled the agents to pinpoint the location of Mr. Lambis's cell phone. They knocked on the door to the apartment, obtained consent from Mr. Lambis's father and entered the home. Ultimately, the agents secured Mr. Lambis's consent to search his room and discovered narcotics, packing material, digital scales and drug paraphernalia. Mr. Lambis moved to suppress the evidence. Relying on the Supreme Court's decision in *Kyllo v. United States*, 533 U.S. at 40, this Court found that the agents had conducted an unreasonable search in violation of the Fourth Amendment. *Lambis*, 197 F.Supp.3d at 610.

Kyllo concerned the use of a thermal imaging device. Federal agents suspected that Kyllo was growing marijuana in his house. Knowing that marijuana growers often

use high-intensity lamps that emit a significant amount of heat, the agents, sitting in a vehicle across the street, used a thermal-imaging device to scan the inside of Mr. Kyllo's home for hot spots. Without ever entering the house, agents discovered that certain parts of the structure were unusually warm. Based on the result of the imaging and other information they had, agents obtained a warrant to search Mr. Kyllo's home. In executing the warrant, they discovered more than 100 marijuana plants. Mr. Kyllo's motion to suppress was denied, and he entered a conditional plea that permitted him to appeal the suppression decision. The Ninth Circuit ultimately affirmed, finding that Mr. Kyllo had no reasonable expectation of privacy because the imaging didn't expose "any intimate details of Kyllo's life, only amorphous hot spots on his home's exterior." *Kyllo*, 535 U.S. at 27

The Supreme Court disagreed, finding that a search had occurred. Its holding was grounded in two concerns. First, the Court emphasized that the officer had "engaged in more than naked-eye surveillance." *Id.* at 33. Advances in technology could not be permitted to "erode the privacy guaranteed by the Fourth Amendment." *Id.* at 34. Second, the intrusion, although not physical, penetrated a home, the area where Fourth-Amendment protection is at its strongest. *Id.* at 35. These factors led to the Supreme Court's conclusion that when "the Government uses a device that is not in general use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search,' and it is presumptively unreasonable without a warrant." *Id.* at 40.

This Court applied the same reasoning in *Lambis*, finding that "the DEA's use of the cell-site simulator to locate Lambis's apartment was an unreasonable search

because the 'pings' from Lambis's cell phone to the nearest cell-site were not readily available 'to anyone who wanted to look' without the use of a cell-site simulator. *Lambis*, 197 F.3d at 610. Noting that "if the Government had wished to use a cell-site simulator, it could have obtained a warrant[ ]," this Court suppressed the evidence.

In granting suppression in *Lambis*, this Court rejected the government's argument that the third-party doctrine developed by the United States Supreme Court in *Smith v. Maryland*, 442 U.S. 735, 742-44 (1979), and *United States v. Miller*, 425 U.S. 435, 441-43 (1976), governed. The *Miller-Smith* line of cases stand for the proposition that a person can have no reasonable expectation of privacy in information he "voluntarily" turns over to third parties.

The Supreme Court first addressed this issue in *Miller*. The government was investigating Miller for tax evasion, and, as part of its investigation, subpoenaed his bank records, including several months of cancelled checks, deposit slips and monthly account statements. Miller sought to suppress the evidence but declined to assert either ownership or possession of the documents. The Supreme Court found that Miller's disavowal of an interest in the records coupled with the fact that the documents were exposed to bank employees in the ordinary course of business deprived him of any reasonable expectation of privacy in the material. *Miller*, 425 U.S. at 433.

The issue arose again three years later in *Smith*. There the government used a pen register to obtain records of telephone numbers Mr. Smith had dialed on a landline, which connected him to a robbery. His motion to suppress was denied, and he was convicted on a trial by stipulated facts. Mr. Smith appealed the suppression decision to the Maryland Court of Appeals, which affirmed his conviction. The United States

Supreme Court granted *certiorari* and held that the use of the pen register did not constitute a search. The Court's decision was influenced by a pen register's limited capabilities and the supposition that it was unlikely that "people in general entertain[ed] any actual expectation of privacy in the number they dial." *Smith*, 442 U.S. at 742. However, the ruling rested on the fact that when Smith placed a call, he voluntarily conveyed the numbers to the phone company (by dialing the numbers). The Court concluded that by doing so he assumed the risk that the company's records would be divulged to the police. *Id*. at 745.

In *Lambis*, this Court, noted that the third-party doctrine was not apt. In reality, cell phone users do not actively submit their information to their service providers. *Id*. at 615. Referring to Justice Sotomayor's concurrence in *United States v. Jones*, 565 U.S. at 400, this Court questioned whether the third-party even retained its doctrinal support in "the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Lambis*, 197 F.3d at 614. Id. at 615. However, this Court found it unnecessary to resolve the question because Mr. Lambis had not voluntarily turned over his information. The government had taken it.

> Nevertheless, the arguments that can be made for the application of the third party doctrine to CSLI do not extend to the distinct technology used by a cell-site simulator, which has an additional layer of involuntariness. Unlike CSLI, the "pings" picked up by the cell-site simulator are not transmitted in the normal course of the phone's operation. Rather, "cell site simulators actively locate phones by forcing them to repeatedly transmit their unique identifying electronic serial numbers, and then calculating the signal strength until the target phone is pinpointed.

Id., *quoting States v. Andrews*, 227 Md.App. 350, 359, n.4, 134 S.3d 224, 324 (2015). Other Courts have also held that use of a cell-site simulator constitutes a search. *United*

States v. Ellis, 270 F.Supp.3d 1134, 1142 (N.D. Cal. Aug. 20, 2017)(cell phone user had a reasonable expectation of privacy in his cell phone location in real time).

Two years after this Court's decision in *Lambis*, the Supreme Court did conclude that the third-party doctrine was not applicable to CSLI in *Carpenter v. United States*, --- U.S. ---, 138 S.Ct. 2206, 2217 (2018). *Carpenter* lends further support for the conclusion that packet sniffing is a search. *See infra* at 30-32. Agent Tarbell, like the agents in *Lambis*, forced the Silk Road server to transmit packet information by repeatedly making entries in the user login interface, using technology that is not in general use. By doing so he conducted a search that required a warrant.

2. Packet Sniffing to Obtain an IP Address is a Search Within the Meaning of the Fourth Amendment to the United States Constitution, Which Requires a Search Warrant

Even if Agent Tarbell obtained no more information than the Silk Road IP address through the packet sniffing, a highly unlikely proposition, his actions violated Mr. Clark's rights under the Fourth Amendment.

Courts, including the Second Circuit, have historically held that an individual does not have a reasonable expectation of privacy in an IP address. *See e.g.*, *United States v. Christie*, 624 F.3d 558, 574 (3rd Cir. 2010); *United States v. Forrester*, 512 F.3d 500, 510-11 (9th Cir. 2009). In fact, in Ross Ulbricht's appeal, the Second Circuit rejected the argument that the government needed a warrant[24] to monitor IP addresses associated with Internet traffic to and from various devices Mr. Ulbricht used. *United States v. Ulbricht*, 858 F.3d 71, 97 (2d Cir. 2017). However, the analysis in those cases, including *Ulbricht*, was grounded in the third-party doctrine, which the United States Supreme

[24]The government had obtained a Pen/Trap Order authorizing it to obtain the information.

Court developed more than forty years ago in *Smith v. Maryland*, 442 U.S. at 742-44, and *United States v. Miller*, 425 U.S. at 441-43. After the Second Circuit decided *Ulbricht,* the Supreme Court disavowed this rationale in Carpenter, 138 S.Ct. at 2213.

Timothy Carpenter was implicated in participating in a string of robberies by a purported co-conspirator. Based on information provided by the cooperator, the government applied for and received two court orders under the Stored Communications Act. The first order authorized the government to obtain 152 days of cell-site location records ("CSLI").[25] The second order covered a seven-day period.[26] Based in part on the information they obtained from the orders, the government charged Mr. Carpenter with Hobbs Act robbery in violation of 18 U.S.C. 1951(a) and with and carrying a firearm during a crime of violence in violation of 18 U.S.C. §924(c). Mr. Carpenter moved to suppress the cell-site data, arguing that the government's seizure required a warrant. The District Court denied suppression. Mr. Carpenter was convicted at trial of all but one of the firearms counts. On appeal he again asserted that the government's use of an order to obtain his CSLI information violated the Fourth Amendment. The Sixth Circuit affirmed on the basis of the third-party doctrine: Because Mr. Carpenter "shared" the information with his wireless carriers, the records the companies generated were not protected by the Fourth Amendment. The United States Supreme Court granted *certiorari* and reversed.

Justice Roberts, writing for the majority, characterized the question before it as "how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the records of a cell phone signal." *Carpenter*, 138

---

[25]The service provider produced records for 127 days.
[26]The service provider produced records for two days.

S.Ct. at 2216. The Court acknowledged that resolution of this issue "implicate[d] the third-party principles of *Smith* and *Miller*." *Id*. A user of a cellphone no less than a user of a landline or a customer of a bank could be said to have revealed to a third-party (his wireless carrier) the information the government sought to gather without using a warrant (his physical location). The Court nevertheless found the third-party doctrine inapplicable. "After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of a person's movement." *Id*. at 2217. Given the advances in technology, the Court concluded that a holding finding that the government's acquisition of CSLI constituted a search was more consistent with the body of case law that had developed since *Smith* and *Miller*. *Carpenter*, 138 S.Ct. at 2219 (finding that rules a Court applies with respect to the Fourth Amendment must take into account sophisticated systems that are already in use or development). Those post-*Smith* cases included *Riley v. California*, 573 U.S. ---, 134 S.Ct. 2473, 2485 (2014), in which the Court held that the police must obtain a warrant to search for digital data in an individual's cellphone; *United States v. Jones*, 565 U.S. 400 (2012), in which five Justices concluded that privacy concerns would be raised by GPS tracking, and *Kyllo v. United States*, 533 U.S. at 35, in which the Court found that the use of a thermal imager to detect heat radiating from the side of the defendant's home was a search. Each decision was predicated on the Court's conclusion that any rule it adopted to cover Fourth Amendment challenges to new technology had to be crafted to "'assure[ ] preservation of that degree of privacy against

government that existed when the Fourth Amendment was adopted.' *Kyllo v. United States*, 533 U.S. 26, 34 (2001)." *Carpenter*, 138 S.Ct at 2214.

In light of *Carpenter*, the Second Circuit's conclusion in *Ulbricht* that an individual does not have a reasonable expectation of privacy in his IP address has lost its conceptual underpinning. While the Second Circuit felt bound by *Smith* and *Maryland* and their progeny to find that Mr. Ulbricht did not have a reasonable expectation of privacy in the IP address of the Silk Road server, *Carpenter* has demonstrated that those cases do not control resolution of this issue. A user of the Internet, like the user of a cellphone, does not "voluntarily" turn over his IP address. Accessing the Internet through a computer is just as a ubiquitous part of life as using a cellphone.

The conclusion that Mr. Clark had a reasonable expectation of privacy in his IP address is further supported by the Pen Register Trap and Trace Act ("Pen Register Act") - 18 U.S.C. §3121 et seq. Under the Act, "[n]o person may install or use a pen register or trap and trace device without first obtaining a court order under section 3132 of this title[.]" 18 U.S.C. 3121(a). A pen register is defined as a "device or process" that "records or decodes" or "captures" the "dialing, routing, addressing, or signal information associated with electronic communications." 18 U.S.C. §3127(3). Packet sniffing indisputably is a device or process that records, decodes or captures routing or addressing information associated with electronic communications.[27] Indeed, the

[27]In *United States v. Contreras*, 905 F.3d 853, 857 (5th Cir. 2018), and *United States v. Hood,* 920 F.3d 87 (1st Cir. 2019), the Fifth and First Circuit Courts of Appeals found that *Carpenter* left unchanged pre-existing Circuit precedent that had held a defendant has no cognizable expectation of privacy in his IP address. It is respectfully submitted that *Contreras* and *Hood*, which are not binding precedent on this Court, were wrongly decided.

government in the Ulbricht prosecution sought several Pen-Trap Orders to obtain information from devices associated with Mr. Ulbricht.

While the Pen Register Act requires the government to obtain an order only, and Mr. Clark asserts that a warrant is required to use a packet sniffer, the Pen Register Act is an indication that society is prepared to recognize as reasonable an individual's expectation of privacy in this type of electronic data.

The government violated the Fourth Amendment by failing to obtain a warrant to engage in packet sniffing.

POINT THREE

THE COURT SHOULD COMPEL THE GOVERNMENT TO PROVIDE ADDITIONAL DISCOVERY

Mr. Clark seeks additional discovery pursuant to Rule 16(E)(i) of the Federal Rules of Criminal Procedure and the Fifth Amendment to the United States Constitution. The information sought relates to the manner in which Agent Tarbell and another member of the CY-2 squad located the Silk Road IP address in "early June" of 2013:

- The name of the software that FBI Special Agent Christopher Tarbell and another member of the Cybercrime Squad ("CY-2") of the New York Field Office of the FBI used to capture packet data sent from the Silk Road server;

- The list of "miscellaneous entries" Agent Tarbell asserts that he or any other member of CY-2 purportedly entered in the username, password and CAPTCHA of the Silk Road login page as part of their attempts in "early June 2013" to locate the Internet Protocol ("IP) address of the Silk Road website;

- All logs or reports that document efforts Agent Tarbell and another member of CY-2 purportedly made in early June of 2013 as part of their efforts to locate the Internet Protocol ("IP) address of the Silk Road website;

- All logs of server-error messages Agent Tarbell and another member of CY-2 purportedly received in early June of 2013 in response to entering invalid data into the Silk Road user login page;

- All valid login credentials Special Agent Tarbell and another member of CY-2 purportedly used as part of their efforts in early June of 2013 to locate the IP address of the Silk Road website;

- All invalid login credentials (user names, passwords and CAPTCHA entries) Special Agent Tarbell and another member of CY-2 purportedly used as part of their efforts in early June of 2013 to locate the IP address of the Silk Road website;

- All packet logs recorded during the course of the Silk Road investigation, including packet logs that showed packet headers containing the IP address of the Silk Road server (193.107.86.49) as of early June of 2013;

- The types of devices Agent Tarbell or other members of CY-2 used in early June of 2013 to obtain the Silk Road IP address;

- All reports, notes, photographs or log files that document the hardware configuration of the Silk Road servers, the Ulbricht laptop and any devices seized from Roger Clark as they existed at the time the images turned over by the government to the defense on July 16, 2018, were made;

- The order of the hard drives in any Redundant Array of Independent Disks (RAID) configuration and any data pertaining to the Basic Input/Output System (BIOS) of the server and other devices images of which were turned over by the government to the defense on July 16, 2018;

- The dates, times and location of the forensic examinations of the Silk Road server;

- Information about how law enforcement obtained the IP address of the initial Silk Road server – 193.107.84.4.

As required by Local Criminal Rule 16.1,[28] co-counsel for Mr. Clark, Jacob Mitchell, sent the government a letter on October 9, 2019, requesting most of the

[28]Local Criminal Rule 16.1 provides as follows: No motion addressed to a bill of particulars or any discovery matter shall be heard unless counsel for the moving party files in or simultaneously with the moving papers an affidavit certifying that counsel has conferred with counsel for the opposing party in an effort in good faith to resolve by

information we now ask the Court to compel the government to disclose. (Mitchell Declaration at ¶19.) On October 17, Mr. Mitchell supplemented his October 9 letter by asking the government provide two additional items. (*Id.*) The government responded by email dated October 23, 2019, and declined to provide any of the material requested. (*Id.* at ¶20.) The government should be required to provide the information.

These items are material for the preparation of the defense. The bulk of what is sought will help defense expert Joshua Michel reach a definitive conclusion on the validity of Agent Tarbell's claims. Based on what he has already reviewed Mr. Michel can state his opinion that it would have been implausible for Agent Tarbell to access the .49 server in the manner he claimed. (Michel Declaration at ¶20.) However, the additional information could enable Mr. Michel to make the servers operational and to repeat the steps Agent Tarbell claimed he took and thereby reach a definitive conclusion about whether Agent Tarbell's Declaration is accurate. The other discovery requests – for the dates, times and locations of the forensic examinations of the Silk Road server and for information on how members of law enforcement discovered the initial Silk Road server (.4) – are also aimed at determining whether Agent Tarbell did or did not tell the truth in his Declaration.

There already is sufficient reason to doubt Agent Tarbell's explanation to justify ordering the government to disclose the requested material. As described in detail throughout this Memorandum, Agent Tarbell provided an extremely vague description of the steps he and his fellow agent supposedly took to uncover Silk Road. Additionally, his explanation raises suspicion. Agent Tarbell is (or was at the time he conduct his

---

agreement the issues raised by the motion without the intervention of the Court and has been unable to reach agreement.

analysis) certified as a Forensic Computer Examiner by both the FBI and the International Association of Computer Investigative Specialist ("IACIS") (Tarbell Declaration at ¶3). Yet, he claims to have kept no records of his activities. His failure to document what he did – he doesn't even know the date he conducted his tests – contravenes the most rudimentary standards of computer forensic analysis and of common sense.

The organization that certified Agent Tarbell as a computer forensic examiner, the IACIS, emphasizes the importance of properly documenting findings. Indeed, some of the "core competencies" individuals must master to be certified by IACIS certification including the following:

a. Knowledge of search and seizure, legal process, and rules of evidence as applicable to computer forensics, laws, and procedures.

b. Ability to explain on-scene actions taken for the preservation of digital evidence.

c. Knowledge of proper computer search and seizure methodologies to include photographic and scene sketch procedures and documentation.

d. Ability to establish, maintain and document a forensically sound examination environment.

(http://www.iacis.com/core competency).

Digital Forensic Examiner Joshua Michel in his Declaration notes the oddity of a forensic computer analyst keeping no records of an examination of a device. Mr. Michel states that "best practices and standards" for analysis of digital information and for reporting the conclusions of that analysis require an examiner to "document actions and procedures" he undertook. (Michel Declaration at ¶¶35-37.) This only makes sense. As Mr. Michel states, recording information aids in the analysis. Additionally, records that document the steps of a digital examination (like all records) also serve as memory

aids. In this case, for example, Agent Tarbell, relying only on his memory, can recall only a very approximate date for when he purportedly conducted his analysis: early June of 2016.

Agent Tarbell's failure to keep records also is at odds with FBI procedure. During the Ulbricht trial, the FBI Special Agent who conducted the initial analysis of Mr. Ulbricht's laptop, Thomas Kiernan, discussed in detail his documentation of his actions:

> [AUSA]: Now, what, if anything, did you do to document what you were doing while you were performing what you were calling the triage of the laptop?
>
> KIERNAN: Sure. I was taking pictures of what I was doing with a BlackBerry, my BlackBerry FBI-issued phone.

(*United States v. Ulbricht*, 14-cr-68 (KFB), excerpt from trial transcript at 859, Exhibit K to Mitchell Declaration.) Agent Kiernan testified that he "didn't do anything at all" before he took the photograph. (*Id.* at 860.) The government introduced at Mr. Ulbricht's trial more than a dozen photographs Agent Kiernan took that documented the steps he took in his analysis of the laptop. When Agent Kiernan conducted a more complete analysis of a forensic image of the computer at a later date, he again took photographs to record what he did. (*Id.* at 878.)

Another aspect of the government's explanation for the discovery of the .49 server is troubling. [redacted] The United States Attorney's Office refused in the Ulbricht prosecution to

provide any information about how this server was located and has declined to do so in this prosecution, while disavowing any intention to rely on information obtained from this server. This raises a question about whether that server was located through lawful means. If it was not, that could give rise to a motion to dismiss the indictment on the grounds of outrageous government conduct. Admittedly, to demonstrate outrageous government conduct that would violate the Due Process Clause of the Fifth Amendment and thereby justify dismissing an indictment, a defendant bears a heavy burden. Courts have generally required a showing that government conduct – by "government" the defense is referring to members of law enforcement, not the United States Attorney's Office – was "so outrageous that common notions of fairness and decency would be offended were judicial processes invoked to obtain a conviction." *United States v. Schmidt,* 105 F.3d 82, 91 (2d Cir. 1997). The challenged conduct must shock the conscience.

There is a reasonable inference to be drawn in these circumstances that some agency of the government obtained the IP address of the initial Silk Road server (.4 server) by illegal means and then lied to the Justice Department about its actions. That version of events was then incorporated by the United States Attorney's Office in filings it made in the Ulbricht prosecution. Certainly, deliberately lying to the Court is outrageous government conduct.

While Agent Tarbell claimed in his Declaration that his discovery of the .49 IP address was completely independent of any examination of the contents of the .4 server, in these highly unusual circumstances, Mr. Clark should not be required to rely on that assertion. *See United States v. Cuervelo*, 949 F.2d 559, 568 (2d Cir.

1991)(finding that District Court erred in not holding a hearing on defendant's claims that undercover DEA agent's initiation of a sexual relationship with her constituted outrageous government conduct that violated her right to due process and warranted dismissal of the indictment. This Court should order the government to provide the requested information.

POINT FOUR

EVIDENCE THAT WAS SEIZED FROM MR. CLARK BY MEMBERS OF THE THAI ROYAL POLICE IS THE FRUIT OF TORTURE AND SHOULD BE SUPPRESSED

Mr. Clark was subjected to torture by member of the Royal Thai Police when they arrested him. Officers came to Mr. Clark's residence on December 3, 2015. They enter his home, restrained him and demanded that he sign a form giving them permission to seize items. (Clark Declaration at ¶21-22.) When he refused to do so, they beat him with sticks. (Id. at ¶23.) He continued to refuse. They continued to beat him. Finally, fearing for his safety, Mr. Clark signed the form, which written in Thai, and wrote in near his signature, "not read or understood, signed under duress." (*Id.*) The officers then seized the following items that belonged to Mr. Clark, which were ultimately turned over to members of law enforcement in the United States:

- The contents of a silver and black Acer Aspire laptop seized from Roger Clark's residence on or about December 3, 2015, (serial number NXM2RST013223110F1200);
- The contents of a silver MacBook Pro laptop seized from Roger Clark's residence on or about December 3, 2015, (serial number C02HN0WNDV7P);
- The contents of a black Hewlett Packard Presario CQ60 with USB dongle inserted seized from Roger Clark's residence on or about December 3, 2015, (serial number 2CE843138V);

- The contents of a Seagate Barracuda LP hard drive seized on or about December 3, 2015, from Roger Clark's residence (Serial number 5YD265A1);

- The contents of a black and blue Transcend thumb drive (8 GB) seized on or about December 3, 2015, from Roger Clark's residence;

- The contents of two Micro Center USB flash drives (32 GB) seized on or about December 3, 2015, from Roger Clark's residence;

- The contents of a dark grey Olympus *fe* camera seized on or about December 3, 2015, from Roger Clark's residence (serial Number J7I20910);

Admission of evidence obtained in this manner would violate the Due Process Clause of the Fifth Amendment.

While suppression generally is not required when the evidence a defendant moves to exclude was obtained by members of foreign law enforcement agencies; *United States v. Getto*, 729 F.3d 221, 227 (2d Cir. 2011); an exception to that rule is applicable in this case. If the evidence was obtained under circumstances that are so extreme that they "shock the judicial conscience", suppression is warranted. *United States v. Maturo*, 982 F.3d 57, 60-61 (2d Cir. 1992). Courts have more often found that contested conduct did not shock the judicial conscious. However, the Second Circuit has indicated that "torture or terror" of a suspect would meet this standard.So would "rubbing pepper in the eyes or other shocking conduct." *Getto*, 729 F.3d at 229 (internal quotation marks and citations omitted).

The case law that has developed in the related context of a defendant seeking to suppress a coerced statement is instructive. One of the justifications for excluding confessions that were induced by physical or psychological compulsion is the concern that a statement obtained through those might not be true. However, "the constitutional

principle of excluding confessions that are not voluntary does not rest on this consideration." *Rogers v. Richmond*, 365 U.S. 540, 541 (1961). Confessions that are obtained through physical or even psychological coercion are suppressed because admitting the evidence "would run contrary to fundamental principles of liberty and justice which lie at the base of our civil and political institutions." *United States v. Ahmed*, 94 F.Supp.3d 394, 436 (E.D.N.Y. 2015)(internal quotations mark and citations omitted). The statement is inadmissible "because due process is violated when "a defendant had been subjected to pressures to which, under our accusatorial system, an accused should not be subjected [.]" *Rogers*, 365 U.S. at 541.

Essentially, the "shocks the judicial conscience standard is meant to protect against conduct that violates fundamental international norms of decency." *Getto*, 729 F.3d at 229. Beating someone with sticks – repeatedly – certainly meets this standard. The physical evidence seized from Mr. Clark must be suppressed.

CONCLUSION

For all the reasons stated herein and in the accompanying Notice of Motion and Declarations, the Court should suppression the evidence obtained directly and indirectly as a result of the search of the Silk Road servers that were discovered in Iceland, suppress the physical evidence that was seized from Mr. Clark at his home in Thailand and order the government to provide additional discovery.

Respectfully submitted,

_____/s/_____
Stephanie M. Carvlin

cc: Assistant United States Attorneys:
Michael Neff
Vladislav Vainberg
Eun Young Choi (VIA ECF)